Chicago Public Schools Policy Manual

Title: **INFORMATION SECURITY POLICY**
Section: **102.7**
Board Report: 19-0828-PO1 **Date Adopted:** August 28, 2019

Policy:

THE CHIEF EXECUTIVE OFFICER RECOMMENDS:

That the Board amend Board Report 13-0925-PO1 Information Security Policy.

The purpose of these amendments is to:

1) give the newly created role of Director of Information Security the authority to create standards for Security and Privacy Controls of CPS Information Systems, and
2) clarify that the Chief Information Officer and Director of Information Security will develop, establish and implement District-wide information security measures using NIST 800-53 and other contemporary industry standards, guidance and protocols relevant to the unique information privacy and security concerns of educational institutions.

PURPOSE: The purpose of this policy is to authorize the Chief Information Officer and the Director of Information Security to develop, establish and implement District-wide information privacy and security measures using the *NIST (National Institute of Standards and Technology) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations* and other state-of-the-art standards, guidance and protocols relevant to the unique information private and security concerns of educational institutions in order to: (1) protect the confidential information maintained in District's data, systems, and electronic records from unauthorized disclosure including, but not limited to, student and employee information, operational plans, and financial information; (2) protect against security breaches and system attacks while allowing business processes to function on a continuous, uninterrupted basis with reasonable assurance that the data and information has not been altered; and (3) protect against the misuse or improper use of the District's information resources to a level that protects the Board while still allowing day-to-day functions.

POLICY TEXT:

A. Security and Privacy Controls

The Chief Information Officer ("CIO") or the Director of Information Security (DIS) shall assess the District's systems threats and vulnerabilities and develop, establish and implement appropriate control measures to protect electronic data and information resources commensurate to the risk of adverse events. The CIO or DIS shall develop, establish and revise as necessary District-wide standards, requirements, procedures and control measures using NIST 800-53 and other contemporary industry standards, guidance and protocols relevant to the unique needs of educational institutions, specifically in the following areas:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Asset Monitoring and Tracking
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- Component Authenticity
- System and Communications Protection
- Port and I/O Device Access
- System and Information Integrity

The control measures established by the CIO or DIS should address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance with applicable federal and state data privacy and security laws, and procedures to facilitate the implementation.

B. Violations

Failure to abide by this Policy or standards, guidelines, procedures or control measures issued by the CIO or DIS will subject employees or students to discipline up to and including dismissal in accordance with Board Rules and Policies.

Any Board contractor, consultant, or other business partner who violates this policy may have their system access privileges suspended and may be further subject to contract termination or any other remedy or action deemed appropriate by the Board.

Amends/Rescinds:	Amends 13-0925-PO1
Cross References:	04-0825-PO3 (Adopted September 22, 2004)
Legal References:	